On Near Prime-Order Elliptic Curves with Small Embedding Degrees

Duc-Phong Le, Nadia El Mrabet, Tan Chik How

On near prime-order elliptic curves with small embedding degrees

Duc-Phong Le*
Temasek Laboratories
National University of Singapore
tslld@nus.edu.sg

Nadia El Mrabet
SAS team CMP
Ecole des Mines de St Etienne
nadia.el-mrabet@emse.fr

Chik How Tan
Temasek Laboratories
National University of Singapore
tsltch@nus.edu.sg

Abstract

In this paper, we generalize the method of Scott and Barreto in order to construct a family of pairing-friendly elliptic curve. We present an explicit algorithm to obtain generalized MNT families curves with any cofactors. We also analyze the complex multiplication equations of these curves and transform them into generalized Pell equation. As an example, we describe a way to generate Edwards curves with embedding degree 6.

Keywords: Pairing Friendly Elliptic Curve, MNT curves, Complex Multiplication, Pell's equation.

1 Introduction

Pairings used in cryptology are efficiently *computable* bilinear maps on torsion subgroups of points on an elliptic curve that map into the multiplicative group of a finite field. We call such a map a *cryptographic pairing*. The first notable application of pairings to cryptology was the work of Menezes, Okamato and Vanstone [14]. They showed that the discrete logarithm problem on a supersingular elliptic curve can be reduced to the discrete logarithm problem in a finite field through the Weil pairing. Then, Frey and Ruck [9] also consider this situation using the Tate pairing. Pairings were thus used as a means of attacking cryptosystems.

However, pairings on elliptic curves only become a great interest since their first application in constructing cryptographic protocols in [12], which describes an one-round 3-party Diffie-Hellman key exchange protocol in 2000. Since then, the use of cryptographic protocols based on pairings has had a huge success with some notable breakthroughs such as practical Identity-based Encryption (IBE) schemes [6], short signature schemes [5]. At high level, a pairing is a bilinear and non-degenerate map $e : \mathbb{G}_1 \times G_2 \to G_3$, with G_1 and G_2 two subgroups of order r of an elliptic curve E and G_3 a subgroup of a finite field. Unlike standard elliptic curve cryptosystems, pairing-based cryptosystems require elliptic curves with special properties, namely, the embedding degree k is small enough. Let q be a prime number or a power of a prime, let E be an elliptic curve defined over $\mathbb{F}_q$ with a subgroup of prime order r. Then the embedding degree is the smallest integer such that r divides $(q^k - 1)$. This ensures that cryptographic pairings are *computable* over the extension finite field. An elliptic curve with such nice properties is called a *pairing-friendly* elliptic curve.

Miyaji, Nakabayashi and Takano introduced the concept of "family of pairing-friendly elliptic curves" in [16]. They provided families of *prime-order* elliptic curves with embedding degrees $k = 3, 4$ and 6, that is, the number of points on these curves $E(\mathbb{F}_q)$ are prime. As analyzed in [17], these families of curves, so-called MNT curves, are more efficient than supersingular elliptic curves when implementing pairing-based cryptosystems. Later, Scott and Barreto [18], and Galbraith *et al.* [10] extended and introduced more MNT curves. These curves are of *near prime-order*, that is, curves with small cofactors $h \geq 2$. The number of points on these curves is $\#E(\mathbb{F}_q) = h \cdot r$, where r is prime. While Galbraith *et al.*'s method allows generating explicit families of curves, Scott-Barreto's method generates only particular elliptic curves.

In this paper we extend the method of Scott and Barreto in [18] and present an explicit, simple algorithm to generate families of ordinary elliptic curves of prime order (or near prime order with any cofactor) with small embedding degrees. We then point out a one-to-one correspondence between families of MNT curves having the same embedding degree and the same cofactor (Theorems 4.2, 4.4, and 4.6). We also analyze the complex multiplication equations of these curves and show how to transform these complex multiplication equations into

*Contact author

generalized Pell equations that allow us to find particular curves. We illustrate our analysis for constructing Edwards curves with embedding degree 6.

The paper is organized as follows: Section 2 briefly recalls MNT curves, as well as methods to generate MNT curves with small cofactors. Section 3 presents an alternative method to generate such curves. We give our results in Section 4. We also discuss the Pell equation for some particular cases of MNT curves in this section. Finally, we conclude in Section 5.

2 Backgrounds

2.1 MNT curves

An elliptic curve generated randomly would have a large embedding degree. As a consequence, a random elliptic curve would not be suitable for efficient computation of a pairing based protocol. Supersingular elliptic curves have small embedding degree. However, such curves are limited to embedding degree $k = 2$ for prime fields and $k \leq 6$ in general [15]. If we want to vary the embedding degree to achieve a high security level, we must construct *pairing-friendly ordinary elliptic curves*. However, a study by Balasubramanian and Koblitz in [2] showed that ordinary elliptic curves with such a small embedding degree are *very rare* and thus require specific constructions.

In [8], the authors give a taxonomy of existing constructions and families of pairing-friendly elliptic curves. They define precisely what a parameterization of a pairing friendly elliptic curve is.

Definition 2.1 (Freeman-Scott-Teske, [8], Definition 2.7) *Let $t(x)$, $r(x)$, and $q(x)$ be nonzero polynomials with rational coefficients.*

(i) For a given positive integer k and a positive square-free integer D, the triple (t, r, p) parameterizes a family of elliptic curves with embedding degree k and discriminant D if the following conditions are satisfied:

1. *$q(x) = p(x)^d$ for some integer $d \geq 1$ and $p(x)$ a polynomial representing primes.*
2. *$r(x)$ is non-constant, irreducible, integer-valued and has positive leading coefficient.*
3. *$r(x)$ divides $q(x) + 1 - t(x)$.*
4. *$r(x)$ divides $\Phi_k(t(x) - 1)$, where Φ_k is the k^{th} cyclotomic polynomial.*
5. *The equation $D \cdot y^2 = 4q(x) - t(x)^2$ has infinitely many integer solutions (x, y).*

If these conditions are satisfied, we often refer to the triple (t, r, p) as a family.

(ii) For (t, r, q) as in (i), if x_0 is an integer and E is an elliptic curve over $\mathbb{F}_q(x_0)$ with trace $t(x_0)$, then we say E is a curve in the family (t, r, q).

(iii) We say that a family (t, r, q) is ordinary if $gcd(t(x), q(x)) = 1$.

(iv) We say that a family (t, r, q) is complete if there is some $y(x) \in \mathbb{Q}[x]$ such that $D \cdot y(x)^2 = 4q(x) - t(x)^2$; otherwise we say that the family is sparse.

(v) We say that (t, r, q) parameterizes a potential family of curves if conditions (2)–(5) of (i) are satisfied; in this case $p(x)$ may or may not represent primes.

The integer $t(x)$ represent the trace of the elliptic curve over $\mathbb{F}_{p(x)}$ with prime order $r(x)$.

The construction of elliptic curve is based on the Complex Multiplication method (CM for short). The most interesting construction of pairing-friendly elliptic curves is the one such that the result is a parameterization of a family of elliptic curve. Using the CM method of elliptic curve, the ρ value verifies that $1 \leq \rho \leq 2$, where the value ρ is defined as $\rho = \frac{\log(q)}{\log(r)}$. In order to save bandwidth during the calculation we are looking for ρ as small as possible.

Miyaji, Nakabayashi, and Takano presented the first parameterized families that yield ordinary elliptic curves with embedding degree $k \in \{3, 4, 6\}$ [16]. These curves have a ρ-value equals to 1. The families are given by parameterization for q and t as polynomials in $\mathbb{Z}[x]$ with $\#E(\mathbb{F}_q) = n(x)$. We recall that $n(x) = q(x) + 1 - t(x)$, $n(x) | \Phi_k(q(x))$, and $n(x)$ represents primes in the MNT construction. Their results are summarized in Table 1.

k	$q(x)$	$t(x)$
3	$12x^2-1$	$-1 \pm 6x$
4	x^2+x+1	$-x$ or $x+1$
6	$4x^2+1$	$1 \pm 2x$

Table 1: Parameters for MNT curves [16]

Remark : The above families of elliptic curves when $k = 3, 6$ can be simplified by performing a $\mathbb{Z}$-linear change of variable $2x \mapsto x$. We will use $\mathbb{Z}$-linear transformations to simplify our construction of elliptic curves, and also to find more MNT curves with our method.

The construction of MNT curve is based on the Complex Multiplication method (CM for short). That is, we have to find solutions (x_0, V_0) in the following CM equation:

$$DV^2 = 4q(x) - t^2(x)$$

for small values of D. The right-hand side of this equation is of quadratic form and can be transformed into a generalized Pell equation. Since construction depends on solving a Pell-like equation, MNT curves of prime order are *sparse* [8]. It means that the equation admits only a few solutions.

2.2 MNT curves with small cofactors

Let $E(\mathbb{F}_q)$ be a parameterized elliptic curve with cardinality $\#E(\mathbb{F}_q) = n(x)$. We call the cofactor of $E(\mathbb{F}_q)$, the integer h such that $n(x) = h \times r(x)$, where $r(x)$ is a polynomial representing primes. The original construction of MNT curves gives family of elliptic curves with cofactor equals to 1. Scott-Barreto [18], and Galbraith-McKee-Valença [10] extended the MNT idea by allowing small values of cofactor $h > 1$. This allows to find many more suitable curves with $\rho \approx 1$ than original MNT construction. Let $\Phi_k(x)$ is the k-th *cyclotomic polynomial*, we have the following proposition.

Proposition 2.1 *[8, Proposition 2.4] Let k be a positive integer, $E(\mathbb{F}_q)$ be an elliptic curve defined over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t = hr$, where r is prime, and let t be the trace of $E(\mathbb{F}_q)$. Assume that $r \nmid kq$. Then $E(\mathbb{F}_q)$ has embedding degree k with respect to r if and only if $\Phi_k(q) \equiv 0 \pmod{r}$, or equivalently, if and only if $\Phi_k(t-1) \equiv 0 \pmod{r}$.*

2.2.1 Scott-Barreto's method

Let $\Phi_k(x) = dr$ for some x. Scott-Barreto's method [18] first fixes small integers h and d and then substitute $r = \Phi_k(t-1)/d$, where $t = x + 1$ to obtain the following CM equation:

$$DV^2 = 4h\frac{\Phi_k(x)}{d} - (x-1)^2. \tag{1}$$

Actually, Scott and Barreto used the fact that $\Phi_k(t-1) \equiv 0 \pmod{r}$. As above, the right-hand side of the equation 1 is quadratic, hence it can be transformed into a generalized Pell equation by a linear substitution (see [18, §2] for more details). Then, Scott-Barreto found integer solutions to this equation for small D and arbitrary V with the constraint $4h > d$. Note that the Scott-Barreto's method [18] did not give explicit families of elliptic curve, but particular elliptic curves.

2.2.2 Galbraith McKee and Valença's method

Galbraith, McKee and Valença [10] generalized the MNT analysis and gave a complete characterization of curves with small cofactors h. We denote their method by GMV. Similarly to the method in [16], Galbraith *et al.* use the fact that $\Phi_k(q) \equiv 0 \pmod{r}$. They then defined λ by the equation $\Phi_k(q) = \lambda r$. For example, in the case $k = 6$, they required $\lambda r = \Phi_k(q) = q^2 - q + 1$. Then, they applied the same idea as in [16] to seek the explicit families of pairing-friendly elliptic curves. That is, they used the Hasse's bound, $|t| \leq 2\sqrt{q}$, to derive possible solutions q, t from the equation $\Phi_k(q) = \lambda r$. Readers are referred to [10, Section 3] for a particular analysis in the case the embedding degree $k = 6$ and the cofactor $h = 2$.

3 An alternative approach to Galbraith *et al.*'s method

In this section, we present an alternative approach to generate explicit families of ordinary elliptic curves with embedding degree $3, 4$, or 6 and small cofactors. Different from analytic approach in [10], we obtain families of curves by presenting very simple and explicit algorithms. Our analyses also show that these algorithms can find all families of elliptic curves of small embedding degrees with any given cofactor.

3.1 Preliminary observations and facts

Some well-known facts and observations that can be used to find families of curves are noted in this section. Similar to Scott-Barreto's method, we use the fact that $\Phi_k(t-1) \equiv 0 \bmod r$. Consider cyclotomic polynomials corresponding to embedding degrees $k = 3, 4, 6$:

$$\begin{aligned}\Phi_3(t(x)-1) &= t(x)^2 - t(x) + 1,\\ \Phi_4(t(x)-1) &= t(x)^2 - 2t(x) + 2,\\ \Phi_6(t(x)-1) &= t(x)^2 - 3t(x) + 3.\end{aligned}$$

By setting $t(x) = ax + b$, we have the following equations:

$$\Phi_3(t(x)-1) = a^2x^2 + a(2b-1)x + \Phi_3(b-1), \tag{2}$$
$$\Phi_4(t(x)-1) = a^2x^2 + 2a(b-1)x + \Phi_4(b-1), \tag{3}$$
$$\Phi_6(t(x)-1) = a^2x^2 + a(2b-3)x + \Phi_6(b-1). \tag{4}$$

Theorem 3.1 *Quadratic polynomials $\Phi_3(t(x)-1)$, $\Phi_4(t(x)-1)$ and $\Phi_6(t(x)-1)$ are irreducible over rational field.*

Proof We start with the following lemma.

Lemma 3.2 *Let $f(x)$ be a quadratic irreducible polynomial in $\mathbb{Q}[x]$. If we perform any $\mathbb{Z}$-linear change of variables $x \mapsto ax+b$ for any $a \in \mathbb{Q}\setminus\{0\}$ and $b \in \mathbb{Q}$, $f(x)$ will still be a quadratic irreducible polynomial in $\mathbb{Q}[x]$.*

Proof If we assume that $f(ax+b)$ is not irreducible in $\mathbb{Q}[X]$, then as $f(x)$ is a quadratic polynomial it means that $f(ax+b)$ admits a decomposition of the form $f(ax+b) = c(x-c_1)(x-c_2)$, for $c, c_1, c_2 \in \mathbb{Q}$. The values c_1 and c_2 are rational roots of $f(ax+b) = 0$. It is easy to see that $ac_1 + b$ and $ac_2 + b$ would then be rational root of $f(x) = 0$. ∎

We now prove Theorem 3.1. As the polynomial $\Phi_3(x) = x^2 - x + 1$ is irreducible in $\mathbb{Q}[x]$, according to Lemma 3.2 the polynomial $\Phi_3(t(x)-1)$ is also irreducible in $\mathbb{Q}[x]$. The same argument ensures that $\Phi_4(t(x)-1)$ and $\Phi_6(t(x)-1)$ are irreducible in $\mathbb{Q}[x]$. ∎

Let a triple (t, r, q) parameterize a family of generalized MNT curves, and let h be a small cofactor. Let $n(x)$ be a polynomial representing the cardinality of elliptic curves in the family (t, r, q). That is, $n(x) = h \cdot r(x) = q(x) - t(x) + 1$. By Definition 2.1, we have:

$$\Phi_k(t(x)-1) = m \cdot r(x), \tag{5}$$

where $m \in \mathbb{Z}$, and $r(x)$ is a quadratic irreducible polynomial. From e Equations (2)–(4), it is clear to see that m is the greatest common divisor of the coefficients appearing in these equations. For instance, when $k = 3$, m is the GCD of $\Phi_3(b-1)$, a^2, and $a(2b-1)$. We recall the following well-known Lemma, which can be found in [11, Chapter V, §6]:

Lemma 3.3 *Let m be prime and $k, n > 0$. If m divides $\Phi_k(n)$, then m does not divide n, and either m divides k or $m \equiv 1 \pmod{k}$.*

Example In the case of $k = 6$, suppose that $\Phi_6(ax+b') = m \cdot r(x)$, where $b' = b - 1$. Then m will be the greatest common divisor of a^2, $a(2b'+1)$ and $\Phi_6(b')$, and either $m|6$ or $m \equiv 1 \pmod 6$.

From the following definition, we observe that the simplest form of $t(x)$ we can choose is $a = m$.

Definition 3.1 *Let $r(x)$, $r'(x)$, $t(x)$ and $t'(x)$ be polynomials. We say that a pair $(t(x), r(x))$ is* equivalent *to $(t'(x), r'(x))$ if we can transform the first into the second by performing an $\mathbb{Z}$-linear change of variables $x \mapsto cx + d$.*

By Hasse's bound, $4q(x) \geq t^2(x)$, we get the inequality

$$4h \geq m \tag{6}$$

Due to the bound of m as given in the inequality (6), our algorithms could make a brute-force search to find all possible families of elliptic curves for any cofactor h. In principle, our method works as follows:

1. We first fix the Frobenius trace to be $t(x) = ax + b$, for $a \in \mathbb{Z} \setminus \{0\}$ and $b \in \mathbb{Z}$. The maximum of a for a given cofactor h is determined by the inequality 6.
2. Then, we determine m and $r(x)$ thanks to the equation (5).
3. For given m and $r(x)$, we determine $n(x)$ and $q(x)$.

We describe our method by explicit algorithms in following sections. Readers also can find an implementation of our algorithms in MAGMA [7] in Appendix A.

3.2 The proposed algorithm

Algorithm 1 describes our method to obtain a list of pair $(m, r(x))$. Given an embedding degree k and a maximum value of the coefficient a of polynomial $t(x)$, Algorithm 1 outputs a list of polynomials representing prime orders of subgroup of points.

Algorithm 1: Get a list of $r(x)$

Input: k, h_{max}, b_{max}.
Output: List of $t(x), r(x), q(x)$ and corresponding cofactor h for the embedding degree k.

$L \leftarrow \{\}$; $T \leftarrow \{\}$;
$a_{max} = h_{max}$;
for $a = -a_{max}$ **to** a_{max} **do**
  for $b = -b_{max}$ **to** b_{max} **do**
    $t(x) \leftarrow ax + b$;
    $f(x) \leftarrow \Phi_k(t(x) - 1)$;
    Let $f(x) = m \cdot r(x)$, where $m \in \mathbb{Z}$ and $r(x)$ is an irreducible quadratic polynomial;
    if *pair* $(t(x), r(x))$ *is not* equivalent *with any* $(t'(x), r'(x))$ *in* T **then**
      $T \leftarrow T + \{(m, t(x), r(x))\}$;
      for $h = \lceil m/4 \rceil$ **to** h_{max} **do**
        $q(x) \leftarrow h \cdot r(x) + t(x) - 1$;
        if $q(x)$ *is irreducible and* $gcd(q(x), r(x) : x \in \mathbb{Z}) = 1$ **then**
          $L \leftarrow L + \{(t(x), r(x), q(x), h)\}$;
        end
      end
    end
  end
end
return L

The Lemma 3.4 gives the boundary for the value a_{max} in order to find all the possible families of curves.

Lemma 3.4 *Given m, a, b and h corresponding to parameters used in order to generate a family of ordinary elliptic curves. We find the following boundary for the value a_{max} for each embedding degree*

$$k = 3 \rightarrow a_{max} = 4h, \tag{7}$$
$$k = 4 \rightarrow a_{max} = 8h, \tag{8}$$
$$k = 6 \rightarrow a_{max} = 12h. \tag{9}$$

Proof Considering our notations, we have that

$\Phi_k(t(x)-1) = m \times r(x)$

We know that $m \in \mathbb{Z}$ (Equation 5), m is the gcd of factors of $\Phi_k(t(x)-1)$, i.e. m divides a^2, $(2b-1)$ or $2a(b-1)$ or $(2b-3)$ and $\Phi_k(b-1)$ (Equations (2)–(4)), if m divides $\Phi_k(b-1)$ then m does not divide $(b-1)$ and either m divides k eitheir $m \equiv 1 \mod (k)$ Lemma 3.3.

In our case we have that m divides a^2. If m is square free, then we have that m divides a and as a consequence we can choose a_{max} to be $4h$. But, if m is not square free, then $m = p^2 \times m'$ with p a prime number greater or equal to 2. Than we can deduce that p divides a. We are going to investigate for each value of the embedding degree a boundary for a_{max}.

$\mathbf{k = 3}$: As p divides $\Phi_3(b-1) = b^2 - b + 1$ and p divides $2b-1$ we have that p divides $(2b-1) + \Phi_3(b-1)$, i.e p divides $b(b-1)$. We know that p does not divide $(b-1)$, then we have p divides b.

Consequently, if p divides $2b-1$ and b then p must divides -1 which is contradictory with the hypothesis of p being a prime number greater than 2. It means that for $k = 3$, the value of m is square free and the boundary for a_{max} is $4h$.

$\mathbf{k = 4}$: We have that p divides $2(b-1)$. But, we know that m does not divide $(b-1)$ so p does not divide $(b-1)$.

Then, if $(b-1)$ is even, then p cannot divide 2 and we obtain a contradiction, so m is square free.

If $(b-1)$ is odd, then p divides 2. Then a nice boundary for a_max would be $2 \times 4h = 8h$.

$\mathbf{k = 6}$: Like for $k = 3$, as p divides $\Phi_6(b-1) = b^2 - 3b + 3$ and $2b-3$ we have that p divides $(2b-3) + \Phi_3(b-1) = b(b-1)$. We know that p does not divide $(b-1)$, then we have p divides b.

But if p divides $2b-3$ and p divides b then p must divides $2b - 3 + b = 3(b-1)$, then p divides 3. As a consequence, a boundary for a_max would be $3 \times 4h = 12h$. ∎

Algorithm 1 outputs a list of the simplest form of polynomials $(t(x), r(x), q(x))$ for cofactors $h \leq h_{max}$. In the following section, we present our results for curves having embedding degrees $k = 3, 4, 6$.

4 More near prime-order elliptic curves

The families of elliptic curves we obtained are presented in Tables 2, 3, and 4. Our algorithms execute an *exhaustive search* based on the given parameters, they can thus generate *all* families of elliptic curves of small embedding degrees 3, 4 and 6 with any cofactor. In the Tables 2, 3 and 4, we present only families of curves with cofactors $1 \leq h \leq 6$, but it is worth to note that a family of curves with any cofactor can be easily found by adjusting parameters of the algorithms implemented in Appendix A.

4.1 k = 3

For the case of $k = 3$, our results are summarized in Table 2. We don't claim new explicit families in comparison to results in [10]. Our families of curves in the Table 2 can be obtained due to a linear transform of variables from the Table 3 in [10] when $k = 3$. For example, for $h = 2$, our family $q(x) = 2x^2 + x + 1$, and $t(x) = -x$ is equivalent to the family $q(x) = 8x^2 + 2x + 1$, and $t(x) = -2x$ in [10, Table 3]. Our algorithm just gives the polynomials $r(x)$ and $q(x)$ with the least value of coefficients. We also point out one-to-one correspondence between families of curves having the same cofactor h as in Proposition 4.2.

Theorem 4.1 *Table 2 gives all families of elliptic curves of the embedding $k = 3$ with different cofactors $1 \leq h \leq 6$.*

Proposition 4.2 *Let $q(x), r(x)$ and $t(x)$ be non-zero polynomials that parameterize a family of curves with embedding degree $k = 3$ and small cofactor $h \geq 1$. Then $q'(x) = q(x) - 2t(x) + 1$, $r(x)$, and $t'(x) = 1 - t(x)$ represent a family of curves with the same group order $r(x)$ and the same cofactor h.*

Proof Let $q(x), r(x)$ and $t(x)$ parameterize a family of curves with embedding degree $k = 3$, the small cofactor $h \geq 1$, and let $n(x) = h \cdot r(x)$ represent the number of points on this family of curves. We have $\Phi_3(t(x)-1) = t(x)^2 - t(x) + 1$. Now,

$$\Phi_3(t'(x)-1) = \Phi_3(-t(x)) = t(x)^2 - t(x) + 1 \tag{10}$$

$$= \Phi_3(t(x)-1). \tag{11}$$

h	q	r	t
1	$3x^2-1$	$3x^2+3x+1$	$-3x-1$
2	$2x^2+x+1$	x^2+x+1	$-x$
	$14x^2+3x-1$	$7x^2+5x+1$	$-7x-2$
	$14x^2+17x+4$	$7x^2+5x+1$	$7x+3$
3	$3x^2+2x+2$	x^2+x+1	$-x$
4	$4x^2+3x+3$	x^2+x+1	$-x$
	$12x^2+9x+2$	$3x^2+3x+1$	$-3x-1$
	$28x^2+13x+1$	$7x^2+5x+1$	$-7x-2$
	$28x^2+27x+6$	$7x^2+5x+1$	$7x+3$
5	$5x^2+4x+4$	x^2+x+1	$-x$
	$35x^2+18x+2$	$7x^2+5x+1$	$-7x-2$
	$35x^2+32x+7$	$7x^2+5x+1$	$7x+3$
	$65x^2+22x+1$	$13x^2+7x+1$	$-13x-3$
	$65x^2+48x+8$	$13x^2+7x+1$	$13x+4$
	$95x^2+56x+7$	$19x^2+15x+3$	$-19x-7$
	$95x^2+94x+22$	$19x^2+15x+3$	$19x+8$
6	$6x^2+5x+5$	x^2+x+1	$-x$
	$18x^2+15+4$	$3x^2+3x+1$	$-3x-1$
	$78x^2+29x+2$	$13x^2+7x+1$	$-13x-3$
	$78x^2+55x+9$	$13x^2+7x+1$	$13x+4$
	$114x^2+71x+10$	$19x^2+15x+3$	$-19x-7$
	$114x^2+109x+25$	$19x^2+15x+3$	$19x+8$
	$126x^2+33x+1$	$21x^2+9x+1$	$-21x-4$
	$126x^2+75x+10$	$21x^2+9x+1$	$21x+5$

Table 2: Valid q, r, t corresponding to $k = 3$

Since $r(x)|\Phi_3(t(x)-1)$, we have that $r(x)|\Phi_3(t'(x)-1)$ and $q(x) = n(x)+t(x)-1$. Now,

$$q'(x) = q(x) - 2t(x) + 1 \tag{12}$$
$$= n(x) - t(x) \tag{13}$$
$$= n(x) + t'(x) - 1. \tag{14}$$

It is easy to see that $q'(x)$ is the image of $q(x)$ by a $\mathbb{Z}$-linear transformation of $t(x) \mapsto 1 - t(x)$. According to Lemma 3.2, since $q(x)$ is irreducible then $q'(x)$ is irreducible. Let $n'(x) = n(x)$, then $q'(x)$ represent the characteristic of the family of curves.

Now we need to prove that $q'(x)$ and $t'(x)$ satisfies the Hasse's theorem, i.e. $t'(x)^2 \leq 4q'(x)$. Suppose that $t(x) = ax + b$, then $t'(x) = -ax - b + 1$. It is clear that the leading coefficient of $q'(x)$ is equal to that of $q(x)$. Since $h > m/4$, $4q(x)$ would be greater than $t^2(x)$ for some value of x. Thus, $q'(x)$ and $t'(x)$ satisfies the Hasse's theorem whenever $q(x)$ and $t(x)$ does with some big enough values of x. ∎

4.2 k = 4

For the case of $k = 4$, our results are summarized in Table 3.

Theorem 4.3 *Table 3 gives families of elliptic curves of the embedding $k = 4$ with small cofactors $1 \leq h \leq 6$.*

It may appear that [10, Table 3] gives more families than ours, but in fact several families of curves with a given cofactor in [10, Table 3] are curves with a higher cofactor, as mentioned in Section 2.2.2. Besides, some families of curves are equivalent by Definition 3.1, e.g., two families $(t, q) = ((-10l-1), (60l^2+14l+1))$ and $((10l+4), (60l^2+46l+9))$ are equivalent. Thus, the number of families they obtained is not as much as they claimed.

We claim new explicit families in comparison to results in [10]. Our new families of curves in the Table 3 cannot be obtained by a linear transform of variables from the Table 3 in [10]. For example, when $h = 5$, we

h	q	r	t
1	x^2+x+1	x^2+2x+2	$-x$
2	$4x^2+2x+1$	$2x^2+2x+1$	$-2x$
3	$3x^2+5x+5$	x^2+2x+2	$-x$
	$15x^2+7x+1$	$5x^2+4x+1$	$-5x-1$
	$15x^2+13x+3$	$5x^2+6x+2$	$-5x-2$
4	$8x^2+6x+3$	$2x^2+2x+1$	$-2x$
5	$5x^2+9x+9$	x^2+2x+2	$-x$
	$25x^2+15x+3$	$5x^2+4x+1$	$-5x-1$
	$25x^2+25x+7$	$5x^2+6x+2$	$-5x-2$
	$65x^2+37x+5$	$13x^2+10x+2$	$-13x-4$
	$65x^2+63x+15$	$13x^2+10x+2$	$13x+6$
	$85x^2+23x+1$	$17x^2+8x+1$	$-17x-3$
	$85x^2+57x+9$	$17x^2+8x+1$	$17x+5$
6	$12x^2+10x+5$	$2x^2+2x+1$	$-2x$
	$60x^2+26x+3$	$10x^2+6x+1$	$-10x-2$
	$60x^2+46x+9$	$10x^2+6x+1$	$10x+4$
	$102x^2+31x+2$	$17x^2+8x+1$	$-17x-3$
	$102x^2+65x+10$	$17x^2+8x+1$	$17x+5$

Table 3: Valid q, r, t corresponding to $k = 4$

present two new families with $t(x) = -5x - 1$ and $t(x) = -5x - 2$. We also reorganize the classification in order to have the correct cofactor in each case. Our algorithm gives the polynomials $r(x)$ and $q(x)$ with the least value of coefficients. We also point out one-to-one correspondence between families of curves having the same cofactor h as in Proposition 4.4.

Proposition 4.4 *Let non-zero polynomials $q(x), r(x)$ and $t(x)$ parameterize a family of curves with embedding degree $k = 4$ and the small cofactor h. Then $q'(x) = q(x) - 2t(x) + 2$, $r(x)$, and $t'(x) = 2 - t(x)$ represent a family of curves with the same embedding degree and the same cofactor.*

Proof The proof of the Proposition 4.4 is similar to that of Proposition 4.2. Assume that $t(x) = ax + b$, and $t'(x) = 2 - t(x)$, we have $\Phi_4(t(x) - 1) = \Phi_4(t'(x) - 1) = t(x)^2 - 2t(x) + 2$.

Similarly, we can get $q'(x) = q(x) - 2t(x) + 2 = n(x) + t'(x) - 1$, where $q'(x)$ is irreducible, and polynomials $t'(x), q'(x)$ satisfy the Hasse's theorem. ∎

4.3 k = 6

As in the case $k = 4$, we find new families of MNT curves compared to GMV's results. These new families are not a transformation by a $\mathbb{Z}$-linear application of existing one. Table 4 gives more explicit families than Table 3 of [10] for $k = 6$. For instance, when $h = 3$, we have one more family of pairing-friendly elliptic curves with $t(x) = -3x$, $q(x) = 9x^2 + 6x + 2$, and $r(x) = 3x^2 + 3x + 1$.

Theorem 4.5 *Table 4 gives families of elliptic curves of the embedding $k = 6$ with different cofactors $1 \leq k \leq 6$.*

Proposition 4.6 *Let non-zero polynomials $q(x), r(x)$ and $t(x)$ parameterize a family of curves with embedding degree $k = 6$ and the small cofactor $h \geq 2$. Then $q'(x) = q(x) - 2t(x) + 3$, $r(x)$, and $t'(x) = 3 - t(x)$ represent a family of curves with the same embedding degree and the same cofactor.*

Proof The proof of the Proposition 4.6 is also similar to that of Proposition 4.2. Assume that $t(x) = ax + b$, and $t'(x) = 3 - t(x)$, we have $\Phi_6(t(x) - 1) = \Phi_6(t'(x) - 1) = t(x)^2 - 3t(x) + 3$.

Similarly, we can get $q'(x) = q(x) - 2t(x) + 3 = n(x) + t'(x) - 1$, where $q'(x)$ is irreducible, and polynomials $t'(x), q'(x)$ satisfy the Hasse's theorem. ∎

h	**q**	**r**	**t**
1	x^2+1	x^2+x+1	$-x+1$
2	$2x^2+x+2$	x^2+x+1	$-x+1$
	$6x^2+3x+1$	$3x^2+3x+1$	$-3x$
3	$3x^2+2x+3$	x^2+x+1	$-x+1$
	$9x^2+6x+2$	$3x^2+3x+1$	$-3x$
	$21x^2+8x+1$	$7x^2+5x+1$	$-7x-1$
	$21x^2+22x+6$	$7x^2+5x+1$	$7x+4$
4	$4x^2+3x+4$	x^2+x+1	$-x+1$
	$28x^2+13x+2$	$7x^2+5x+1$	$-7x-1$
	$28x^2+27x+7$	$7x^2+5x+1$	$7x+4$
	$52x^2+15x+1$	$13x^2+7x+1$	$-13x-2$
	$52x^2+41x+8$	$13x^2+7x+1$	$13x+5$
5	$5x^2+4x+5$	x^2+x+1	$-x+1$
	$15x^2+12x+4$	$3x^2+3x+1$	$-3x$
	$35x^2+18x+3$	$7x^2+5x+1$	$-7x-1$
	$35x^2+32x+8$	$7x^2+5x+1$	$7x+4$
	$65x^2+22x+2$	$13x^2+7x+1$	$-13x-2$
	$65x^2+48x+9$	$13x^2+7x+1$	$13x+5$
	$95x^2+56x+8$	$19x^2+5x+3$	$-19x-6$
	$95x^2+94x+23$	$19x^2+5x+3$	$19x+9$
6	$6x^2+5x+6$	x^2+x+1	$-x+1$
	$18x^2+15x+5$	$3x^2+3x+1$	$-3x$
	$42x^2+23x+4$	$7x^2+5x+1$	$-7x-1$
	$42x^2+37x+9$	$7x^2+5x+1$	$7x+4$
	$78x^2+29x+3$	$13x^2+7x+1$	$-13x-2$
	$78x^2+55x+10$	$13x^2+7x+1$	$13x+5$

Table 4: Valid q, r, t corresponding to $k = 6$

4.4 Solving the Pell Equations

For elliptic curves with embedding degrees $k = 3, 4, 6$ it is clear that the CM equation $DV^2 = 4q(x) - t^2(x)$ is quadratic. Such an equation can be transformed into a generalized Pell equation of the form:

$$y^2 + DV^2 = f.$$

In [18], Scott and Barreto showed how to remove the linear term in the CM equation to get a generalized Pell equation. In this section, we generalize their idea to get Pell equations for families of elliptic curves presented in Tables 2, 3, and 4

Let $t(x) = ax + b$, $\Phi_k(t(x) - 1) = m \cdot r(x)$, where $k = 3, 4, 6$ and $\#E(\mathbb{F}_q) = h \cdot r(x)$. Similarly to the analysis of Scott-Barreto in [18], we make a substitution $x = (y - a_k)/n$ to transform the CM equations to the generalized Pell equations, where

$$a_3 = 2h(2b - 1) - (b - 2)m, \tag{15}$$
$$a_4 = 4h(b - 1) - (b - 2)m, \tag{16}$$
$$a_6 = 2h(2b - 3) - (b - 2)m, \tag{17}$$
$$n = a(4h - m). \tag{18}$$

We set $n' = n/a$, $g = mn'D$ and

$$f_3 = a_3^2 - (n'b)^2 + 4n'(b - 1)(h - m), \tag{19}$$
$$f_4 = a_4^2 - (n'b)^2 + 4n'(b - 1)(2h - m), \tag{20}$$
$$f_6 = a_6^2 - (n'b)^2 + 4n'(b - 1)(3h - m). \tag{21}$$

The CM equation is transformed to its Pell equation

$$y^2 - gV^2 = f_k, \tag{22}$$

where $k = 3, 4$, or 6[1].

In [13], Karabina and Teske investigated the problem on how solve Pell equations of MNT curves. We illustrate our method for $k = 6$ and $h = 4$.

4.4.1 Case $k = 6$ and $h = 4$

Elliptic curves having cofactor $h = 4$ may be put in form $x^2 + y^2 = 1 + dx^2y^2$ with d a non-square integer. Such curves called Edwards curves were introduced to cryptography by Bernstein and Lange [4]. They showed that the addition law on Edwards curves are faster than all previously known formulas. Edwards curves were later extended to the twisted Edwards curves in [3]. Readers also can see [1] for efficient algorithms to compute pairings on Edwards curves.

Now we give some facts to solve Pell equation for Edwards curves with embedding degree $k = 6$. By using Equation 22, we obtain the following Pell equations:

$$y_1^2 - D_1'V^2 = -176, \tag{23}$$
$$y_2^2 - D_2'V^2 = -80, \tag{24}$$
$$y_3^2 - D_3'V^2 = -80, \tag{25}$$
$$y_4^2 - D_4'V^2 = 16, \tag{26}$$
$$y_5^2 - D_5'V^2 = 16, \tag{27}$$

where $y_i = (x - a_i)/b_i$, $D_i' = b_iD$, for $i \in [1, 5]$, and

$$\begin{array}{lllll} a_1 = -7, & a_2 = -19, & a_3 = -26, & a_4 = -4, & a_5 = -17, \\ b_1 = 15, & b_2 = 63, & b_3 = 63, & b_4 = 39, & b_5 = 39. \end{array}$$

[1]Note that we fix the typo in the value of f_k in [18, §2]. Indeed, f_k must be set to $a_k^2 - b^2$ instead of $a_k^2 + b^2$.

Karabina and Teske [13, Lemma 1] showed that if $4|f_k$ then the set of solutions to $y^2 - D'V^2 = f_k$ does not contain any *ambiguous* class, i.e., there exists no primitive solution $\alpha = y + v\sqrt{D'}$ such that α and its *conjugate* $\alpha' = y - v\sqrt{D'}$ are in the same class. Thus, we can see that equations (23)–(27) don't have any solution that contains an ambiguous class. Hence, if equations (23)–(27) have solutions with $y_i \equiv -a_i \bmod b_i$, and a fixed positive square-free integer D_i' relatively prime to b_i, for $1 \leq i \leq 5$ then t, r, q in Table 4 with $h = 4$ represent a family of pairing-friendly Edwards curves with embedding degree 6.

5 Conclusion

In this paper we extended Scott-Barreto's method and presented efficient and simple algorithms to obtain MNT curves with small cofactors. In the Propositions 4.2, 4.4 and 4.6 we point out a one-to-one correspondence between families of MNT curves having the same embedding degree and the same cofactor. If we are given a parameterization of a MNT curves, we can construct another MNT curve using a $\mathbb{Z}$-linear transformation. We leave as an open problem the consequences on the number of MNT curves and the comparison with heuristics on this number. We also analyze the complex multiplication equations of MNT curves and point out how to transform these complex multiplication equations into generalized Pell equations. In addition, we give a method to generate Edwards curves with embedding degree 6.

References

[1] Christophe Arène, Tanja Lange, Michael Naehrig, and Christophe Ritzenthaler. Faster computation of the Tate pairing. *Journal of Number Theory*, 131(5):842–857, 2011.

[2] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the menezes - okamoto - vanstone algorithm. *J. Cryptology*, pages 141–145, 1998.

[3] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards curves. In *Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology*, AFRICACRYPT'08, pages 389–405. Springer Berlin/Heidelberg, 2008.

[4] Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In *Proceedings of the Advances in Crypotology 13th international conference on Theory and application of cryptology and information security*, ASIACRYPT'07, pages 29–50, Berlin, Heidelberg, 2007. Springer-Verlag.

[5] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In Colin Boyd, editor, *ASIACRYPT '01: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security*, ASIACRYPT '01, pages 514–532, London, UK, 2001. Springer-Verlag.

[6] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, pages 213–229. Springer-Verlag, 2001.

[7] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[8] David Freeman, Michael Scott, and Edlyn Teske. A Taxonomy of Pairing-Friendly Elliptic Curves. *J. Cryptol.*, 23:224–280, April 2010.

[9] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comput.*, 62(206):865–874, 1994.

[10] S.D. Galbraith, J.F. McKee, and P.C. Valença. Ordinary abelian varieties having small embedding degree. *Finite Fields and Their Applications*, 13(4):800–814, 2007.

[11] Pierre Antoine Grillet. *Abstract Algebra*. Springer, July 2007.

[12] Antoine Joux. A One Round Protocol for Tripartite Diffie-Hellman. In *ANTS-IV: Proceedings of the 4th International Symposium on Algorithmic Number Theory*, pages 385–394. Springer-Verlag, 2000.

[13] Koray Karabina and Edlyn Teske. On prime-order elliptic curves with embedding degrees k = 3, 4, and 6. In *Proceedings of the 8th international conference on Algorithmic number theory*, ANTS-VIII'08, pages 102–117, Berlin, Heidelberg, 2008. Springer-Verlag.

[14] Alfred Menezes, Scott Vanstone, and Tatsuaki Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In *STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 80–89, New York, NY, USA, 1991. ACM.

[15] Alfred J. Menezes, Tatsuaki Okamoto, and Scott Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993.

[16] Atsuko Miyaji, Masaki Nakabayashi, and Shunzou Takano. New Explicit Conditions of Elliptic Curve Traces for FR-Reduction. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 84(5):1234–1243, 2001.

[17] Dan Page, Nigel Smart, and Frederic Vercauteren. A comparison of mnt curves and supersingular curves. *Applicable Algebra in Engineering, Communication and Computing*, 17(5):379–392, October 2006.

[18] Michael Scott and Paulo S. Barreto. Generating More MNT Elliptic Curves. *Des. Codes Cryptography*, 38:209–217, February 2006.

A Implementations

The following MAGMA code is a simple implementation of the proposed algorithms. The main functions are GetRx() and GetQx(). Function GetRx takes as inputs an embedding degree k and the two parameters ma and mb, where ma and mb are maximum values of coefficients a and b of the trace polynomial $t(x)$. From equation (5) and the inequality $h > m/4$, our heuristics show that ma should be less than $4h$, where h is the maximum co-factor of curves one want to find. Function GetQx takes as inputs a cofactor h, the trace polynomial $t(x)$ and the polynomial $r(x)$ representing the order of the subgroup of points on curves.

```
GetRx := function(k, ma, mb)
  local max, rx, n, i, j, tx, aold, bold, nold, count;
  aold := []; bold := []; nold := []; count := 2;
  Z<x> := PolynomialRing(Integers()); rx := CyclotomicPolynomial(k);
  aold[1] := 1; bold[1] := 1; nold[1] := x^2;
  for i := 1 to ma do
    for a in [-i, i] do
      for j:= 0 to mb do
        for b in [j, -j] do
          tx := a*x + b;
          f := Evaluate(rx, tx - 1);
          if IsIrreducible(f) then
          qx := f + tx - 1;

          if IsBijection(aold, bold, a, b, nold, f, count - 1) eq false then
            if IsIrreducible(qx) then
              printf "MNT curves : nx = %o; qx = %o; tx = %o \n", f, qx, tx;
            else
              printf "Supersingular curves: qx=%o;(f=)rx=%o;tx=%o\n",Factorization(qx),f,a*x+b;
            end if;
            aold[count] := a; bold[count] := b;
            nold[count] := f; count := count + 1;
          end if;

          else
            L := Factorization(f);

            for nx in L do
              if IsBijection(aold, bold, a, b, nold, nx[1], count - 1) eq false then
                if Degree(nx[1]) eq 2 then
                  aold[count] := a; bold[count] := b;
                  nold[count] := nx[1]; count := count + 1;
                else
                  if nx[1]^2 eq f then
                    printf "Supersingular curves: qx=%o;(f=)rx=%o;tx=%o\n",Factorization(qx),f,a*x+b;
                  end if;
```

```
                end if;
              end if;
            end for;
          end if;
        end for; // for b
      end for; // for j
    end for; // for a
  end for; // for i
  return rx;
end function;

GetQx := function(h, rx, tx)
  local qx, nx;
  Z<x> := PolynomialRing(Integers());

  for i := h div 4 to h do
    nx := i*rx;
    qx := nx + tx - 1;
    if IsIrreducible(qx) then
      qx; i;
    else
      L := Factorization(qx);
      for nx in L do
        if Degree(nx[1]) eq 1 and nx[2] eq 2 then
          L;
        end if;
      end for;
    end if;
  end for;
  return qx;
end function;

IsBijection := function(aold, bold, a, b, ax, bx, c)
  local i, tmp, ai, bi, r; r := false;
  Z<x> := PolynomialRing(Integers());
  for i := 1 to c do
    ai:=a div aold[i]; bi:=(b - bold[i]) div aold[i]; tmp:=Evaluate(ax[i], ai*x + bi);
    if tmp eq bx then   return true;
    else     r := false; end if;
  end for;
  return r;
end function;
```